Net-Centric Enterprise Services (NCES)
User Guide

Version 1.0/ECB 1.2

8 September 2006

Revision History

Date	Version	Description
29 July 2005	0.1	Initial Draft
15 August 2005	0.2	Draft
25 August 2005	0.3	Draft
1 September 2005	0.4	Draft
8-13 September 2005	0.5	Added the necessary "install security SDK" to the beginning of all of the "consumer" workflows – added Section 1.4 – Rules of Engagement
19-20 Sept	0.6	Corrections to workflows to point to new document workspace. Fixes for comments from NCES PMO.
26 Sept – 6 Oct	0.7	Corrections to workflows based on developer inputs, NCES Division review, and corrections from "Dry Run" of NCES Support capabilities on 21-23 Sep 05.
21 Nov	0.8	Updates to document to capture DOL Portal modifications and miscellaneous corrections.
17 Jan	1.0	Corrections to non-working links. Clarified workflow instructions. Combined NIPR and SIPR guides. Added new references to the PKI User Guides.
20 July	1.0	Added links to PKI Guides. Updated Service Discovery/ Service Provider Workflow. Updated End User section to reflect new Service Discovery portlet. New information on User/Pass for SIPR. Removed "draft". Removed references to Pilot WG. Updated date/version. Added information on new Collaboration service. Changed all references from ECB 1.1 to ECB 1.2.
7 September	1.0	Replaced figure 2-4 and 2-9 with updated screenshots from the updated website and finalized formatting of the entire paper.

Table of Contents

Table of Figures

Welcome to the Net-Centric Enterprise Services Program

Welcome to the Net-Centric Enterprise Services (NCES) Program. This program represents a critical part of our efforts to develop a set of workable Core Enterprise Services to support net-centricity throughout the Department of Defense (DoD). The NCES Early Capabilities Baseline (ECB) services provide you and your organization with the opportunity to access and use pre-production versions of these services to support your operations while the NCES acquisition program is in its System Development and Demonstration (SDD) phase in preparation for availability of production versions of these services from Managed Service Providers (MSPs).

NCES is making available the following capabilities on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet):

- Portal
- Service Security
- Mediation
- Content Discovery
- Content Delivery
- Service Discovery
- Machine-to-Machine Messaging
- Metadata Discovery
- Enterprise Catalog

This guide introduces end users and software developers to the services available in the ECB. The Web sites referred to in the guide provide detailed user support and technical information to facilitate ECB service usage. Technical support access and availability also are discussed in the guide.

If you have comments or questions, please contact us at nces@cols.disa.mil or nces@cols.disa.smil.mil.

Once again, we are pleased to welcome you to the NCES Program and look forward to working with you and supporting your efforts to become more ‘Net-Centric’.

How to Use This Guide

This guide provides information on how organizations can get involved in the NCES Early Capabilities Baseline (ECB). The ECB establishes an environment of early NCES capabilities in which candidate services are assessed on a continuous basis. Participation gives end users and software developers an early opportunity to test the capabilities of the ECB services and provide feedback to the NCES Program Management Office for future updates to these services.

This guide explains the cycle of activities, or workflows, necessary for participants to (1) learn more about the NCES Program, (2) log on to the Portal (will migrate to Defense Knowledge Online (DKO) in the future), (3) register to participate in the program, (4) acquire ECB documentation, and (5) use ECB services. The guide also provides the workflows necessary for engaging Web service developers and helping them find instructions and tools for building interoperable services.

The guide provides several links to NCES workspaces, such as the Integrated Product Team workspaces supporting NCES program management, and working group workspaces supporting NCES services development. Users must obtain a DoD Public Key Infrastructure (PKI) user certificate to gain access to the Portal.

How This Guide Is Organized

- Section 1 presents general information on the NCES Program and on accessing the Portal. The section guides users through the initial Portal registration process.
- Section 2 presents the steps users must follow to gain access to the workspace containing NCES services and relevant documentation, including an electronic copy of this guide.
- Sections 3 through 6 describe how NCES users (end users, service consumers, service providers, and data providers) can use and integrate with ECB services.
- Section 7 contains contact information on the Help Desk.

1 Introduction

Information on the Net-Centric Enterprise Services (NCES) Program is located at http://www.nces.dod.mil (Unclassified but Sensitive Internet Protocol Router Network [NIPRNet]) and http://www.nces.dod.smil.mil (Secret Internet Protocol Router Network [SIPRNet]).

1.1 Program Overview

The NCES Program will provide a secure, collaborative information sharing environment and unprecedented access to quality decision-quality information through a Service Oriented Architecture (SOA) that enables achievement of the DoD's data strategy. NCES will promote decision-making superiority, thus increasing the mission effectiveness of and enhancing process execution across the DoD. The program is based on an emerging concept at DoD, called "net-centricity," which enables systems to provide the right information to the right people at the right time.

NCES will support new capabilities in all DoD domains, bringing together the promise of Internet technology and the power of DoD. NCES will enable the creation of a marketplace of information sources and services for DoD information. The program represents a different approach for DoD—an approach that is market-based, enterprise-wide, and joint by design. NCES customers include the Warfighter, Intelligence, and Business domains—anyone within the DoD community who needs to share and retrieve information.

The NCES Program provides four product lines:

1. **Enterprise Service-Oriented Architecture (SOA) Foundation:** Enables DoD transformation by providing the core infrastructure that supports information discovery, data and application interoperability, secure collaboration, assessment of service, and data utilization. The core infrastructure will help reduce the complexity of DoD's information technology environment and promote the reuse of existing information technology capabilities.

2. **DoD Enterprise Collaboration:** Provides collaboration and messaging services, such as whiteboard sessions, conferencing sessions, and messaging, as well as a variety of collaboration tools.

3. **Content Discovery & Delivery:** Supports efficient information advertisement, discovery, and delivery.

4. **Portal:** Provides a personalized, user-defined, Web-based presentation that enables secure access to various enterprise services (including information retrieval and posting), collaboration tools, instant messaging (IM), and working groups.

Each product line represents a bundled set of related capabilities that can be leveraged throughout the DoD Global Information Grid (GIG), thus negating the need for multiple DoD Programs of Record (POR) to build redundant functionality.

Access to NCES services is provided through the Portal, as shown in Figure 1-1.

Figure 1-1. Portal

1.2 Portal Registration

The first step for anyone who wants to become involved in the ECB is to register to use the Portal.

Note: The GIG Enterprise Services (GES) Portal has been migrated to the Defense Online Portal. Although some screenshots in this guide contain references to the GES Portal and the DOL Portal, the term “Portal” is used consistently throughout the guide. If you have a current GES Portal/DOL Portal account, you will not need to re-register on the Portal; your account information will remain in the database.

Figure 1-2 illustrates the workflow for registering to use the Portal.

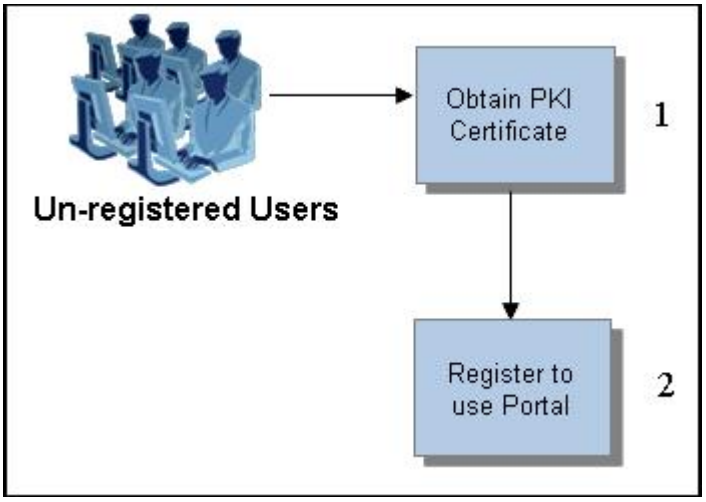

Figure 1-2. Steps for Registering to Use Portal

Step 1. Obtain Public Key Infrastructure (PKI) Certificate

- **NIPRNet:** Please refer to the "NCES PKI User's Guide for NIPRNET/Internet Use" if you are an NCES end user or the "NCES PKI System Administrators and Application Owners Guide for NIPRNET/Internet Use" if you are an NCES service provider or service consumer. These documents can be found on the NCES User Workspace at https://gesportal.dod.mil/sites/NCESPP/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCESPP/default.aspx (SIPRNet).

- **SIPRNet:** Please refer to the "NCES PKI User's Guide for SIPRNET Use" if you are an NCES end user or the "NCES PKI System Administrators and Application Owners Guide for SIPRNET Use" if you are an NCES service provider or service consumer. These documents can be found on the NCES User Workspace at https://gesportal.dod.mil/sites/NCESPP/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCESPP/default.aspx (SIPRNet).

Note: You will need to insert the Common Access Card (CAC) or install the PKI user certificate obtained in Step 1 to complete Step 2.

Step 2. Register to Use the Defense Online Portal

From a Web browser,[1] go to the Portal at https://dol.dod.mil (NIPRNet) or https://dol.dod.smil.mil (SIPRNet). Click on "Defense Online Registration," as shown in Figure 1-3.

[1]Netscape and Firefox support most Portal capabilities; however, use of Internet Explorer is recommended.

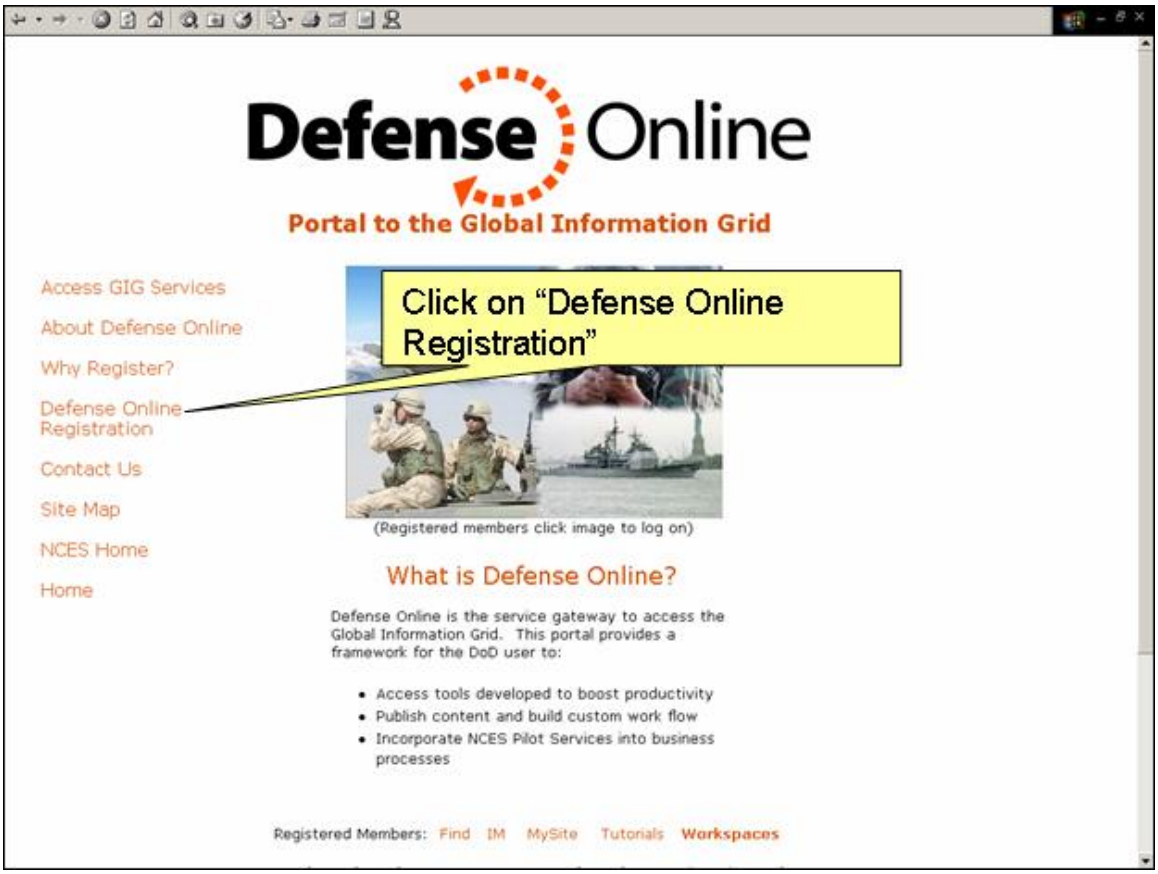

Figure 1-3. Portal Registration

A registration form will appear (see Figure 1-4). Fields are name, email address, phone number, and password. Fill in the required information and click the "Submit" button at the bottom of the page.

Note: Completing the "Audiences" section (not shown in Figure 1-4) of the registration form, which supports user profile development, is optional but beneficial to NCES in evaluating the usefulness of services to our various audiences. Therefore, we would appreciate your additional support by providing this information.

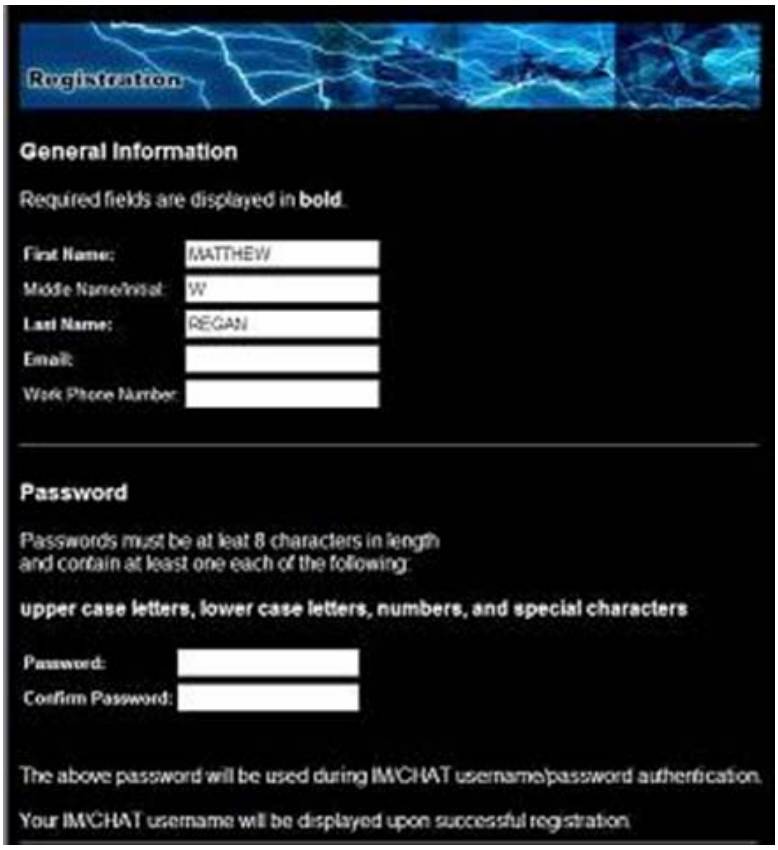

Figure 1-4. Portal Registration Form

A "Registration Successfully Completed" screen will then appear. At this point, you will be able to access the Portal and browse information and workspaces. For more information on using the Portal, see Section 3.1 of this guide.

Note: The user name and password displayed on this screen, which are for the IM client, also can be used to access the SIPRNet Portal after initial registration. A PKI certificate is still necessary for initial registration on the portal.

1.3 NCES Involvement

Members of the DoD community can become involved with the NCES Program in several ways.

- By becoming a User:

  Users are DoD end users and developers who support DoD Programs of Record (PORs) or Communities of Interest (COIs) and can access and use ECB services.

  Note: Developers can be government entities or commercial entities as long as commercial entities directly support a government program.

  Users can engage with NCES in one or more of the following ways:

As an **End User:**
End users can directly access some services, including Portal, Content Discovery and Delivery, and Service Discovery and Registration, via a portal environment.

As a **Service Provider:**
Service providers are developers (government or commercial) that support DoD programs of record and have applications that provide their own services to the enterprise.

As a **Service Consumer:**
Service consumers are developers (government or commercial) that support DoD programs of record and have applications that use/interface with the services provided by NCES.

As a **Data Provider:**
Data providers are developers (government or commercial) that support DoD programs of record and have data to expose to the enterprise.

- By attending **Working-Level Integrated Product Team (WIPT)/Working Group (WG) Meetings**:
  NCES has established WIPTs and lower-level WGs, chaired by NCES or ASD(NII) staff, to engage DoD stakeholders and users. A primary activity of WIPTs and WGs is the review of key acquisition activities and documents. More information on WIPTs and WGs is located at https://gesportal.dod.mil/sites/WIPTsWG/default.aspx .

  WIPTs and WGs meet regularly. Meeting dates and locations, and other information on WIPTs, are posted on the Portal. Attendance is open to representatives of DoD organizations interested in becoming involved in the NCES Program.

  NCES manages or leverages the following WIPTs and WGs. Because of the sensitive information that appears on some of these sites, separate registration may be necessary.

  - **NCES Test & Evaluation WIPT**
    (https://gesportal.dod.mil/sites/NCESTandEWIPT/default.aspx)
    - **Operational Test (OT) WG**
      (https://gesportal.dod.mil/sites/NCESTandEWIPT/otwg/default.aspx)
      - **Mission Thread WG**
        (https://gesportal.dod.mil/sites/NCESTandEWIPT/NCESMissionThreadWorkingGroup/default.aspx)
    - **Early User Test (EUT) 1 WG (ECB)**
    - **Early User Test (EUT) 2 WG (Collaboration)**
    - **Early User Test (EUT) 3 WG (CD&D)**

- **NCES Engineering WIPT** (https://gesportal.dod.mil/sites/NCESENGWIPT/default.aspx)
  - **NCES Architecture WG** (https://gesportal.dod.mil/sites/GES_Architecture_Working_Group/default.aspx)
  - **NCES Content and Storage WG** (https://gesportal.dod.mil/sites/NCES-CS/default.aspx)
  - **SOA Foundation WG** (https://gesportal.dod.mil/sites/SOA_Foundation_WG/default.aspx)
  - **NCES Information Assurance WG** (https://gesportal.dod.mil/sites/nces-ia/default.aspx)
  - **DoD Metadata Registry WG** (https://gesportal.dod.mil/sites/metadata_registry/default.aspx)
  - **Content Discovery and Delivery WG** (https://gesportal.dod.mil/sites/Content_Discovery_WG/default.aspx)
- **NCES Cost WIPT** (https://gesportal.dod.mil/sites/Cost%20WIPT/default.aspx)
- **NCES Acquisition WIPT** (https://gesportal.dod.mil/sites/NCES%20Acquistion%20WIPT/default.aspx)
- **NCES Capabilities Development WG** (https://gesportal.dod.mil/sites/capabilities/default.aspx)

1.4 Rules of Engagement

Users must provide the information discussed in this subsection to the NCES Help Desk (nces@cols.disa.mil or nces@cols.disa.smil.mil), (614) 692-3136, or Defense Switched Network (DSN): 850-3136.

Note: If a user falls into more than one category, he or she only needs to send a single email to the NCES Help Desk that contains the information required for all his or her applicable categories.

1.4.1 End Users

Do not need to provide any information to the Help Desk.

1.4.2 Service Consumers

The organizational representative of a service consumer must provide the following information on the consuming system:

- Mission Assurance Category (MAC), Confidentiality Level (CL), and highest level of data classification (Definitions for MAC and CL are provided in Appendix B.)
- DoD PKI Server Certificate information
- Proof of Authority to Operate (ATO) and Authority to Connect (ATC) with the signature of the system's Designated Approval Authority (DAA)
- Organization's desired outcome of the partnership
- Resources (human and machine) needed from NCES

- Expected number of total and concurrent users accessing NCES
- Time frame for engagement and expected duration
- Performance and reliability requirements
- Machine and domain names

1.4.3 Service Providers

The organizational representative of a service provider must provide the following information on the system:

- MAC, CL, and highest level of data classification
- DoD PKI Server Certificate information
- Proof of ATO and ATC with the signature of the system's DAA
- Web Services Description Language (WSDL) document for registration in the NCES Service Discovery Service
- Organization's desired outcome of the partnership
- Resources (human and machine) needed from NCES
- Expected number of total and concurrent users accessing NCES
- Time frame for engagement and expected duration
- Performance and reliability requirements
- Machine and domain names

1.4.4 Data Providers

The organizational representative of a data provider must provide the following information on the system:

- Classification level of provided data
- DoD PKI Server Certificate information
- Proof of ATO and ATC with the signature of the system's DAA
- Organization's desired outcome of the partnership
- Resources (human and machine) needed from NCES
- Expected number of total and concurrent users accessing NCES
- Time frame for engagement and expected duration
- Performance and reliability requirements
- Machine and domain names

1.5 Glossary

A glossary of NCES Program terms and acronyms is available at http://www.nces.dod.mil/aboutNCES/glossary_content.aspx (NIPRNet) and http://www.nces.dod.smil.mil/aboutNCES/glossary_content.aspx (SIPRNet). A list of acronyms used in this guide is provided in Appendix A.

2 NCES User Access Information

2.1 NCES User Workspace Registration

Once a user has registered to use the Portal (see Section 1.2), they must then follow the steps in this section to gain access to the NCES User Workspace where the link to the NCES Services Interface and relevant NCES documentation can be found. Figure 2-1 illustrates these steps.

Note: The NCES Administrator completes Steps 4, 5, and 6 (indicated in gray type in Figure 2-1).

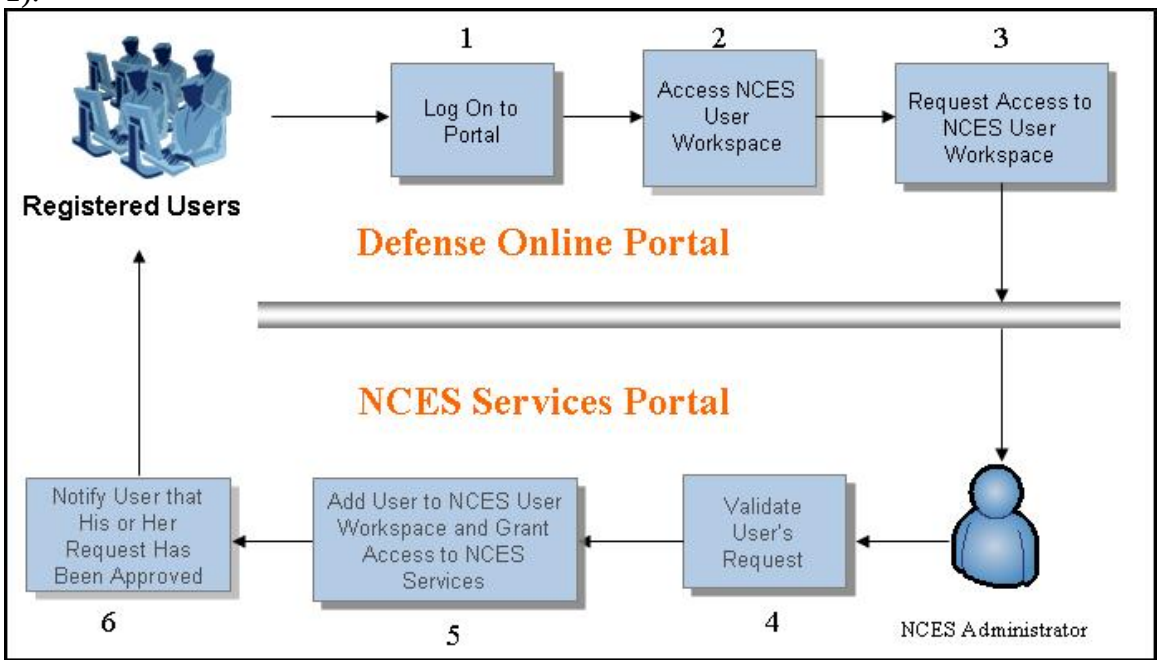

Figure 2-1. Registering to use the NCES User Workspace

Step 1. Log On to Portal

Go to the Portal at https://dol.dod.mil (NIPRNet) or https://dol.dod.smil.mil (SIPRNet). Click on the Warfighter image (see Figure 2-2).

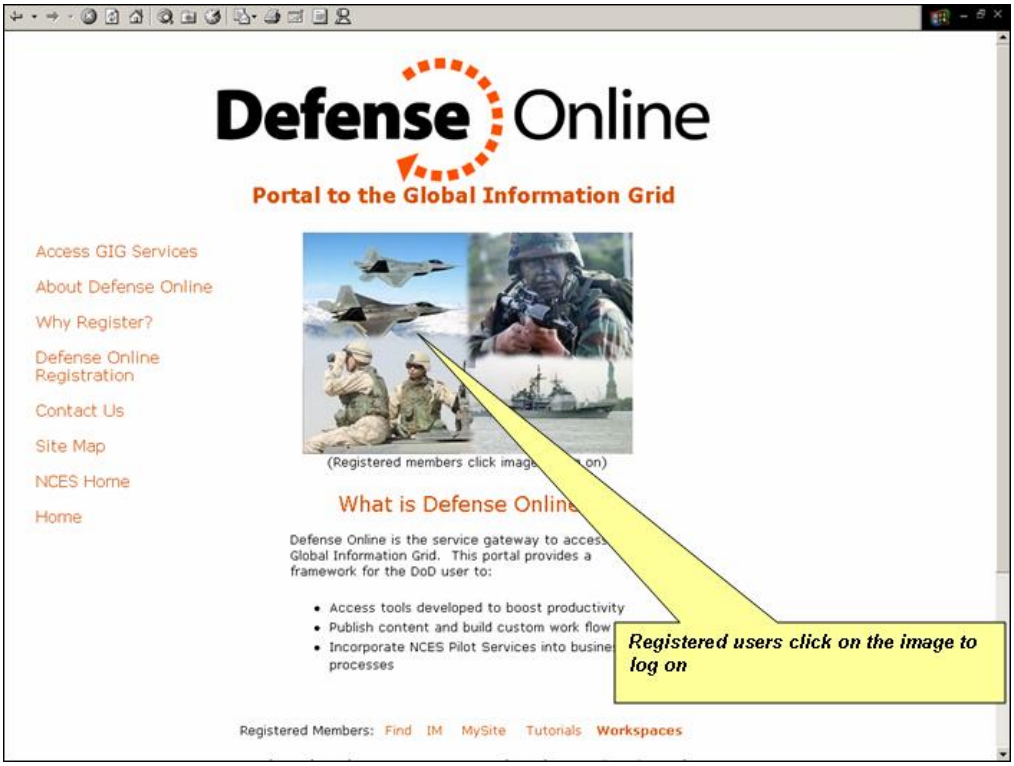

Figure 2-2. Logging On to Portal

The Client Authentication window (see Figure 2-3) will appear (unless you already logged on during a recent session). Select the appropriate PKI user certificate (Identification), click "OK," and enter your Personal Identification Number (PIN).

Note: Your user name and password can be used to access the SIPRNet Portal.

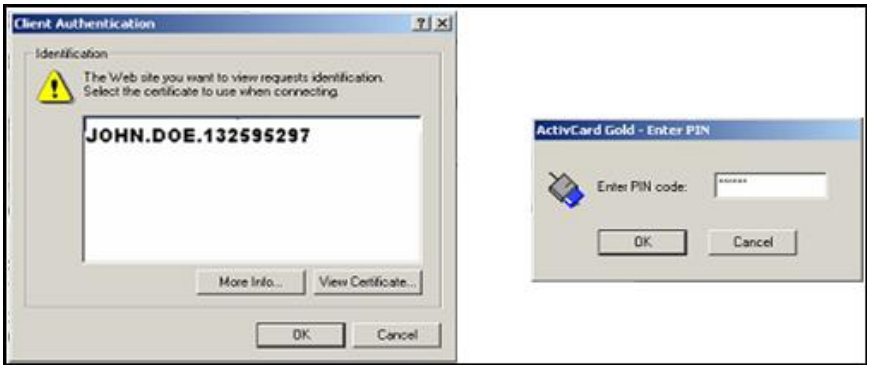

Figure 2-3. Client Authentication Window

Step 2. Access NCES User Workspace

On the Portal home page, click on the "NCES User Workspace" link on the left panel, as illustrated in Figure 2-4.

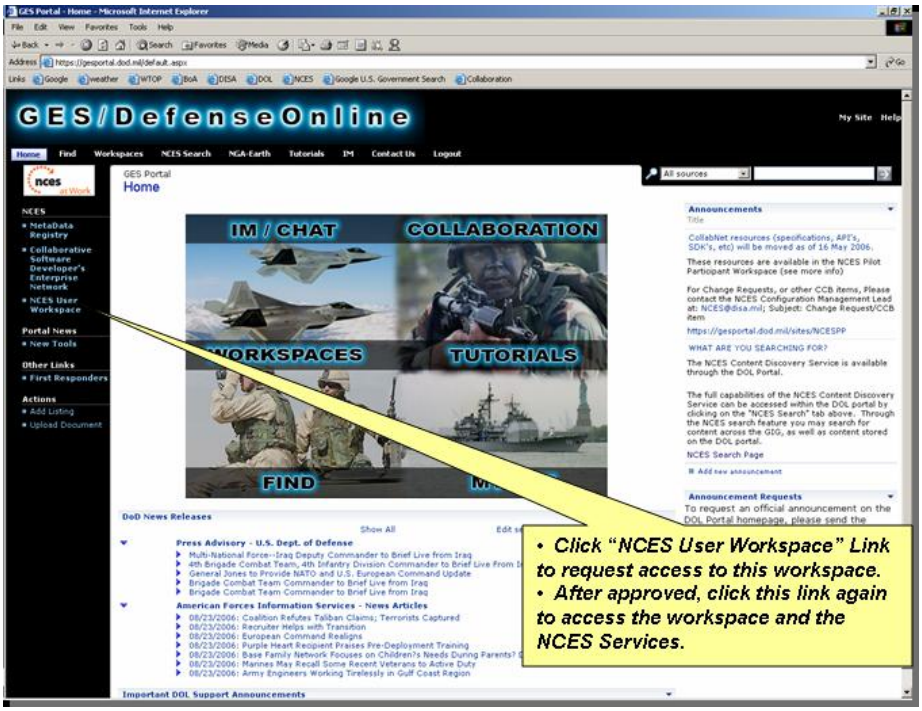

Figure 2-4. NCES User Workspace Link

A NCES User Workspace Registration Form will appear (see Figure 2-5).

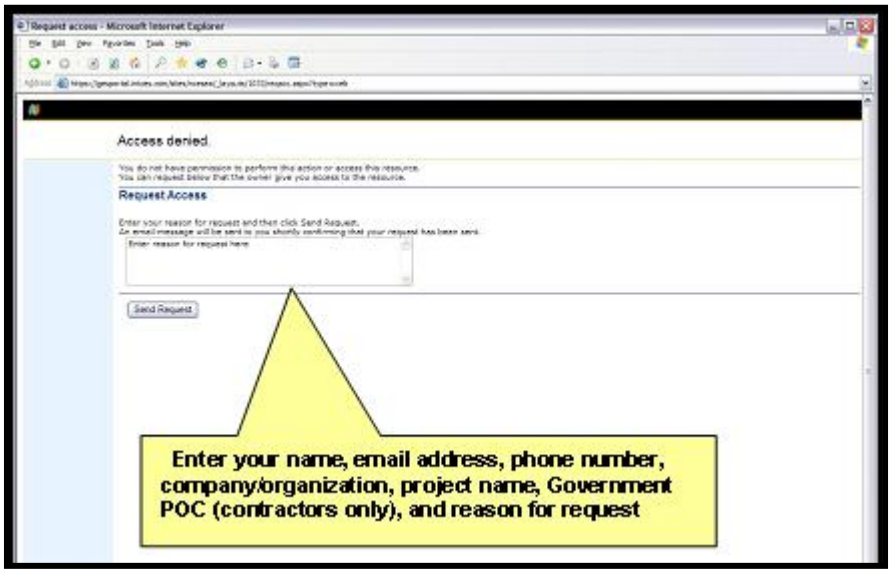

Figure 2-5. NCES User Workspace Registration Form

Step 3. Request Access to NCES User Workspace

Complete the form by providing the following information:

- Name, email address, phone number, company/organization, and project name

- Government point of contact (if you are a contractor)
- Reason for request

Click on the "Send Request" button to send your request to the NCES Administrator for approval.

Note: The NCES Administrator completes Steps 4, 5, and 6.

Step 4. Validate User's Request
Upon receipt of your request, the NCES Administrator will validate your request for approval.

Step 5. Add User to NCES User Workspace and Grant Access to NCES Services Interface
Once your request is approved, the NCES Administrator will add your name to the NCES User Workspace, grant you access to the NCES Services Interface and thus access to NCES services, and add your role to the Lightweight Directory Access Protocol (LDAP) server.

Step 6. Notify User that His or Her Request Has Been Approved
The NCES Administrator will notify you via email within 1 to 3 business days that you have been granted access to the NCES User Workspace and the NCES Services Interface. After you are notified, return to the Portal and log on to the NCES User Workspace by repeating Steps 1 and 2.

2.2 NCES Services Use

Figure 2-6 illustrates the steps you need to take to access the NCES Services Interface and use NCES services.

Note: If virtual private network (VPN) tunneling software is actively running on your PC, you may not be able to access NCES services.

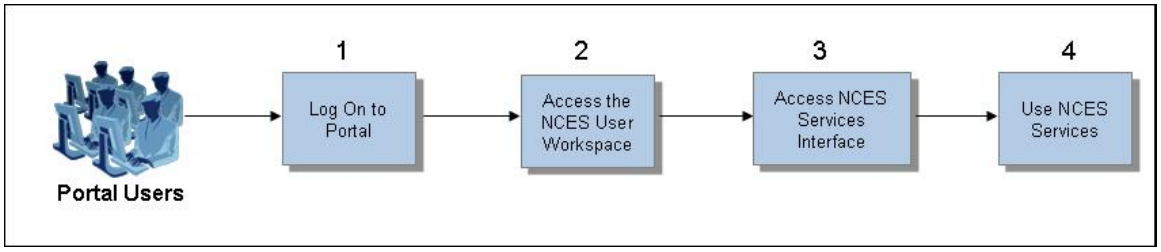

Figure 2-6. Steps for Accessing the NCES Services Interface

Step 1. Log On to Portal
Go to the Portal at https://dol.dod.mil (NIPRNet) or https://dol.dod.smil.mil (SIPRNet). Click on the Warfighter image (see Figure 2-7).

Figure 2-7. Logging On to the Portal

The Client Authentication window (see Figure 2-3) will appear (unless you already logged on during a recent session). Select the appropriate PKI user certificate (Identification), click "OK," and enter your Personal Identification Number (PIN).

Note: Unlike the SIPRNet DOL Portal, the NCES Services Interface will not work with a user name and password; instead, a PKI certificate must be used.

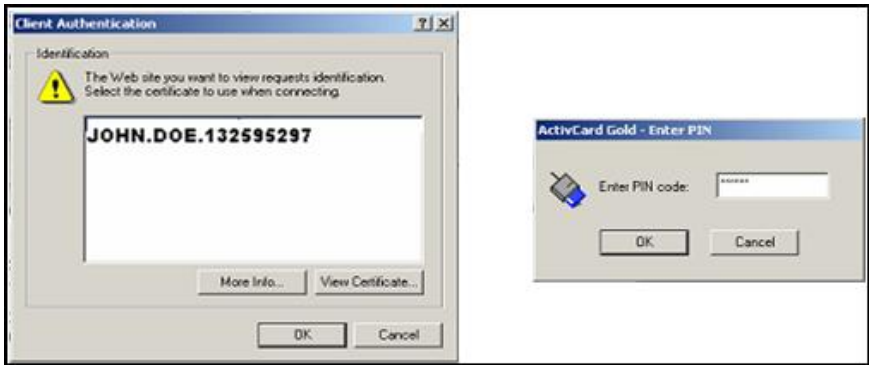

Figure 2-8. Client Authentication Window

Step 2. Access the NCES User Workspace

Click on the "NCES User Workspace" link on the left panel of the Portal home page (see Figure 2-9).

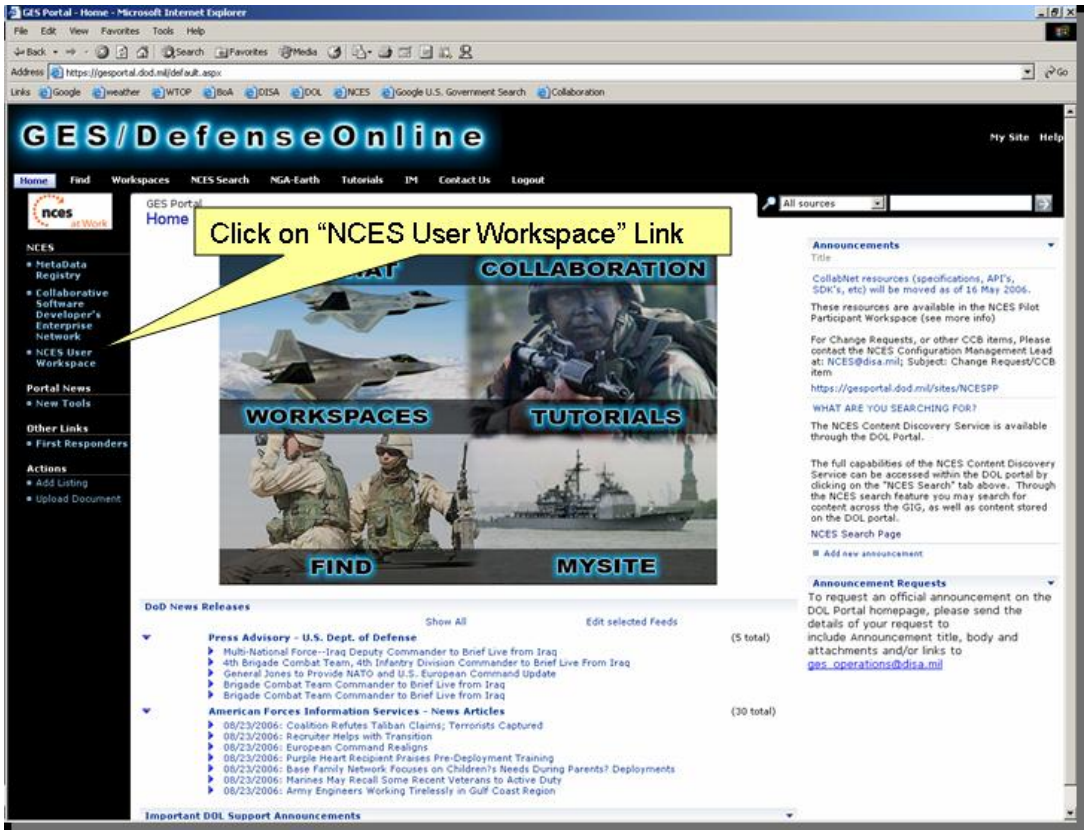

Figure 2-9. "NCES User Workspace" Link

Step 3. Access NCES Services Interface

Click on the "NCES Services Interface" link, as shown in Figure 2-10. Select the PKI user certificate and click "OK." Click on "View Certificate" to determine certificate type. Users must select the PKI identity certificate. The email certificate will not work.

Note: Unlike the SIPRNet DOL Portal, the NCES Services Interface will not work with a user name and password; instead, a PKI certificate must be used.

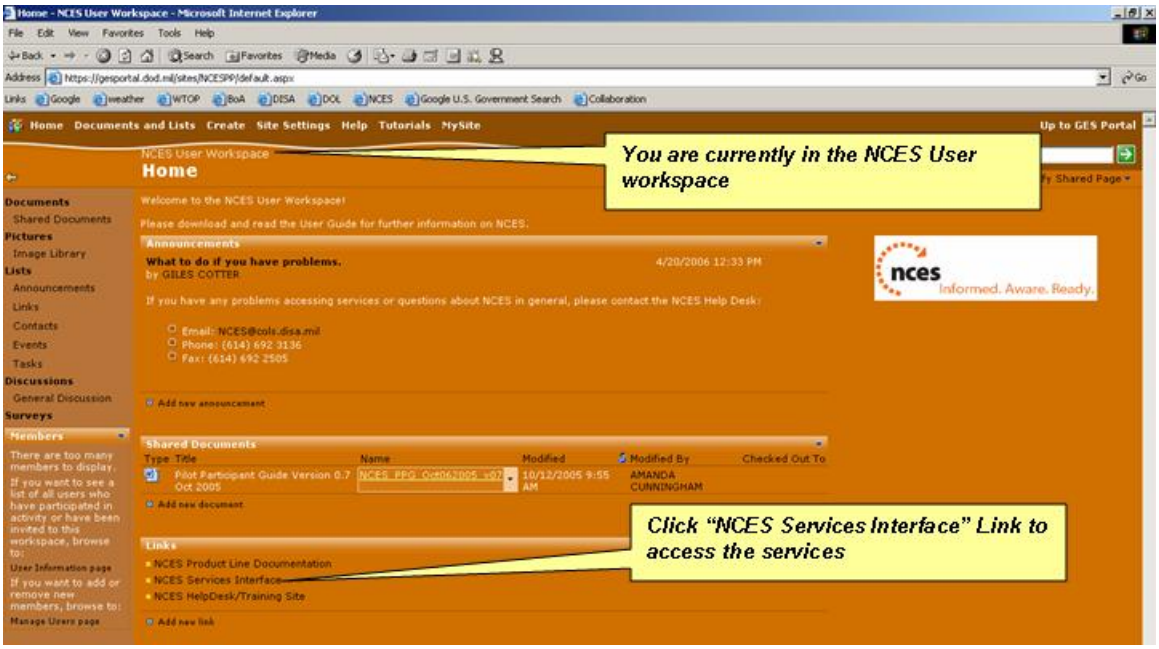

Figure 2-10. "NCES Services Interface" Link

Step 4. Use NCES Services

To use NCES services, place your curser over the "SOA Foundation" or "Content Discovery/Delivery" tabs (see Figure 2-11) to reveal drop-down menus of available services. See Section 3 for information on using the individual services.

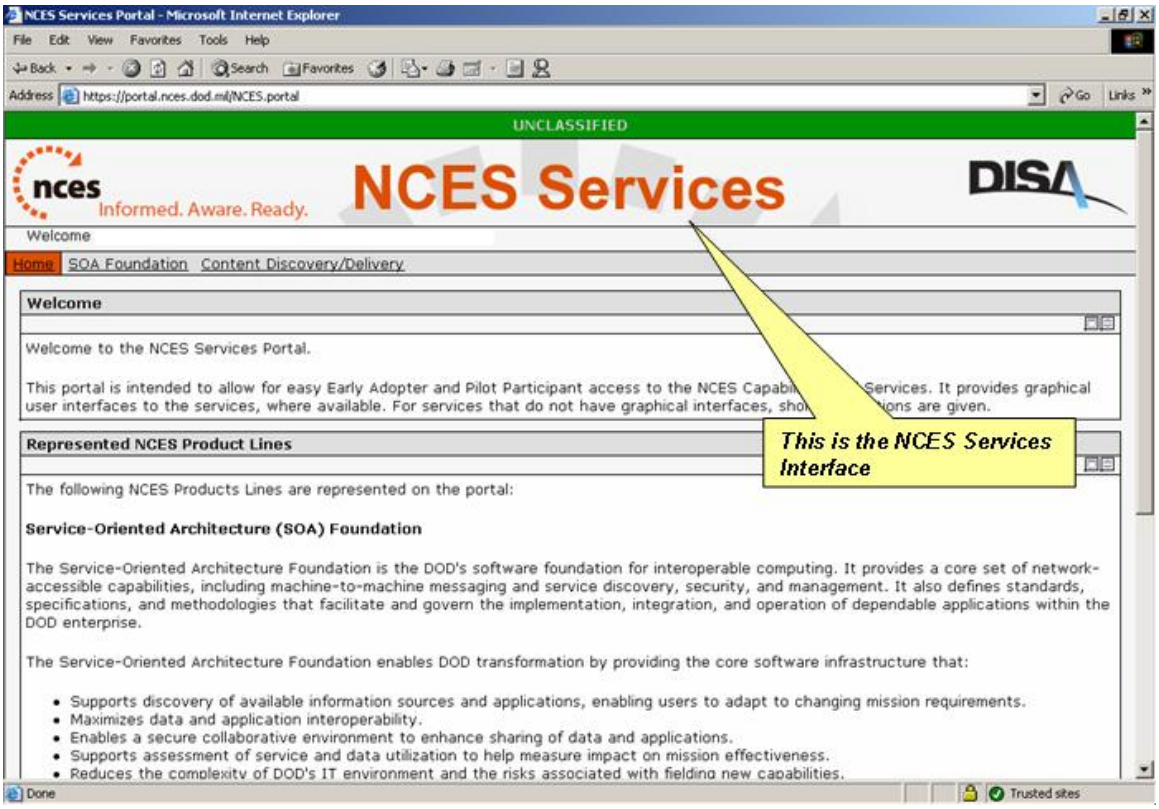

Figure 2-11. NCES Services Interface

3 End User

As an end user, you can directly access certain NCES services, including the following:

- Portal
- Federated Search
- Machine-to-Machine Messaging
- Service Discovery

3.1 Portal

The Portal (https://dol.dod.mil [NIPRNet] or https://dol.dod.smil.mil [SIPRNet]) provides a personalized, user-defined, Web-based presentation that enables secure access to various enterprise services (including information retrieval and posting), collaboration tools, IM, and working groups. For increased security, the Portal integrates with security services. The Portal gives end users access to NCES services and provides a platform to launch these services directly from customer-owned portals. The Portal has several fundamental functions, including Find, Workspaces, Tutorials, and IM.

Note: The Portal will be migrating to the Defense Knowledge Online Portal in the future.

3.1.1 Find

From the Portal home page, you can perform simple searches for people or information by using the search bar at the top right or perform advanced searches according to file type, properties, and date by using the Find function.

3.1.2 Workspaces

You may create your own workspaces to enable you to collaborate with other Portal users by using the Workspace function on the Portal home page. Workspace size is restricted to 250 megabytes. You may access or request access to other workspaces under spotlight sites or by searching for workspaces using the Find function. Type a keyword into the text box and click the arrow key to the right of the box. A list of workspaces containing your keyword will appear. Select a workspace link to access the workspace. You may request access to restricted workspaces from the workspace owner by providing contact information in the form that appears when you attempt to access restricted workspaces.

In addition, you can create a personal Web site, called “MySite,” tailored to your needs. You can customize the appearance of your site and include a number of Web links (e.g., news feeds, weather reports). MySite also offers a place for portal links, customized alerts, and private online storage.

3.1.3 Tutorials

You may access Quick Reference Guides (QRG) by clicking on the “Tutorials” link on the DOL Portal home page. The QRGs provide instructions on the following functions:

- Creating a workspace
- Creating a sub-workspace
- Managing a workspace
- Applying a theme to your workspace
- Editing text within a workspace
- Creating custom security groups within your workspace
- Managing documents within a workspace

The following QRGs provide instructions for creating, editing, and adding Web links to MySite:

- Creating MySite
- Editing MySite
- Using Rich Site Summary (RSS) & Weather within MySite

This QRG explains how to use the Find function efficiently:

- Searching the DOL Portal

The QRGs that follow explain how to use portal tools effectively:

- Using Quick Launch Bar
- Image Library Management
- Using Announcement, Events, and Links
- Using Discussion Boards
- Creating & Using Surveys

3.1.4 Instant Messaging

You can access IM capabilities via the DOL Portal home page. In addition, you can use the Windows Messenger 5.1 Client to communicate with other users by sending and receiving encrypted instant messages. Go to the DOL IM Web page at https://gesportal.dod.mil/IM/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/IM/default.aspx (SIPRNet) for information on IM requirements and capabilities.

3.2 Federated Search

Federated Search is used to query existing data sources, such as databases, catalogs, and search engines, to quickly find stored information. To retrieve content from data sources, submit queries using the NCES Content Discovery Federated Search Portlet (which is accessible using the steps in Section 2.2).

The NCES Content Discovery Federated Search Portlet User Guide provides the steps you need to retrieve content from the GIG and other data sources. The portlet enables you to submit queries to the Federated Search service that will retrieve results from existing data sources. The Advanced Search capability of the Federated Search Portlet enables you to create complex queries to reduce the number of data sources to search, limit searches to certain DoD Discovery

Metadata Specification (DDMS) fields, limit the dates of the documents retrieved, and limit the document types returned. To download the NCES Content Discovery Federated Search Portlet User Guide, go to the NCES Product Line Workspace at https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

Click on "Early Capabilities Baseline (ECB) 1.2 Documents" and select the Federated Search Service folder. The document titled "NCES_CD_FederatedSearchPortlet_UserGuide-Draft" will be listed and can be downloaded.

3.3 Machine-to-Machine Messaging

Machine-to-Machine (M2M) Messaging supports asynchronous notification within the enterprise. Applications, such as the Message Store Portlet, use the M2M Messaging service to deliver alerts and notifications to end users.

The NCES Message Store Portlet User Guide explains how to subscribe to authorized channels and publish messages (which may include one or more attachments) to authorized channels. The Message Store Portlet enables you to subscribe to one or more channels based on your roles. Once subscribed, you will see all messages published to the channel that have not expired and can display these messages and view attachments. To download the Message Store Portlet User Guide go to the NCES Product Line Workspace at https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

Click on "Early Capabilities Baseline (ECB) 1.2 Documents" and select the Machine-to-Machine Messaging folder. The document titled "NCES_M_MessagingStorePortlet_UserGuide" will be listed and can be downloaded.

3.4 Service Discovery

Service Discovery enables users to search for service information in a service registry.

To use this service, access the NCES Services Interface (see Figure 3-1), as shown in Section 2.2. Place your cursor over the "SOA Foundation" tab and select Service Discovery from the drop-down menu.

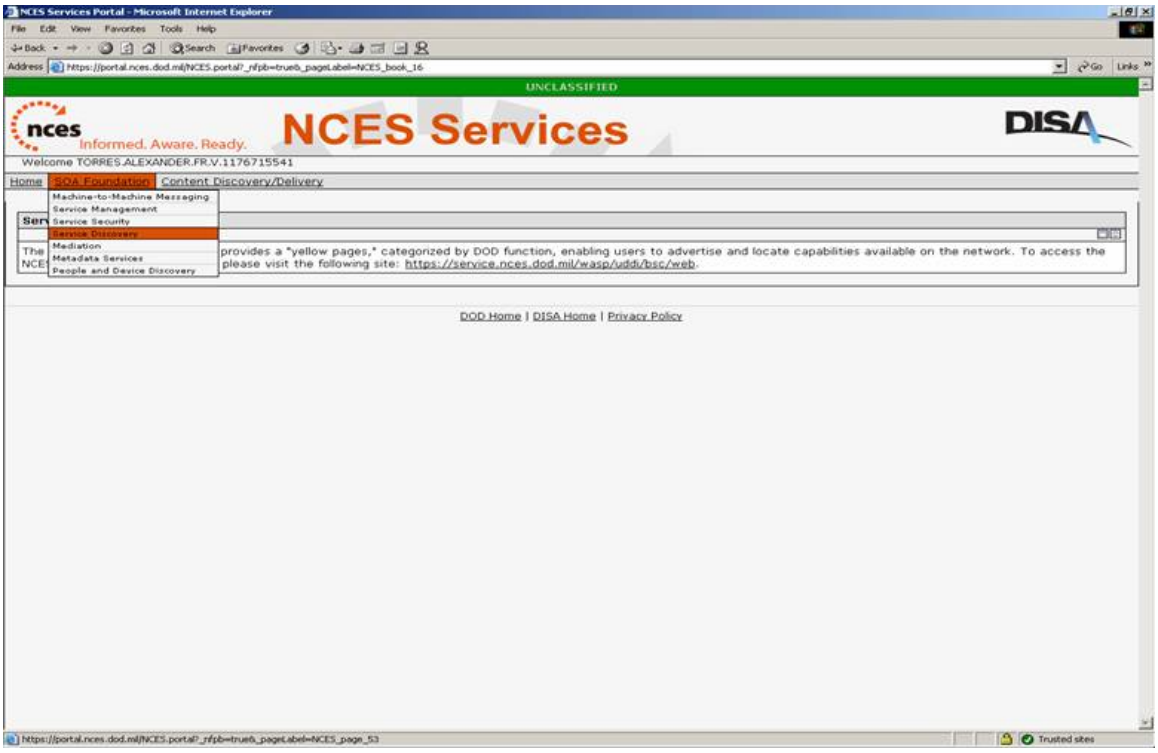

Figure 3-1. NCES Services Interface

Next, click on the link https://service.nces.dod.mil/wasp/uddi/bsc/web (shown in Figure 3-1) to access the NCES Service Registry (shown in Figure 3-2).

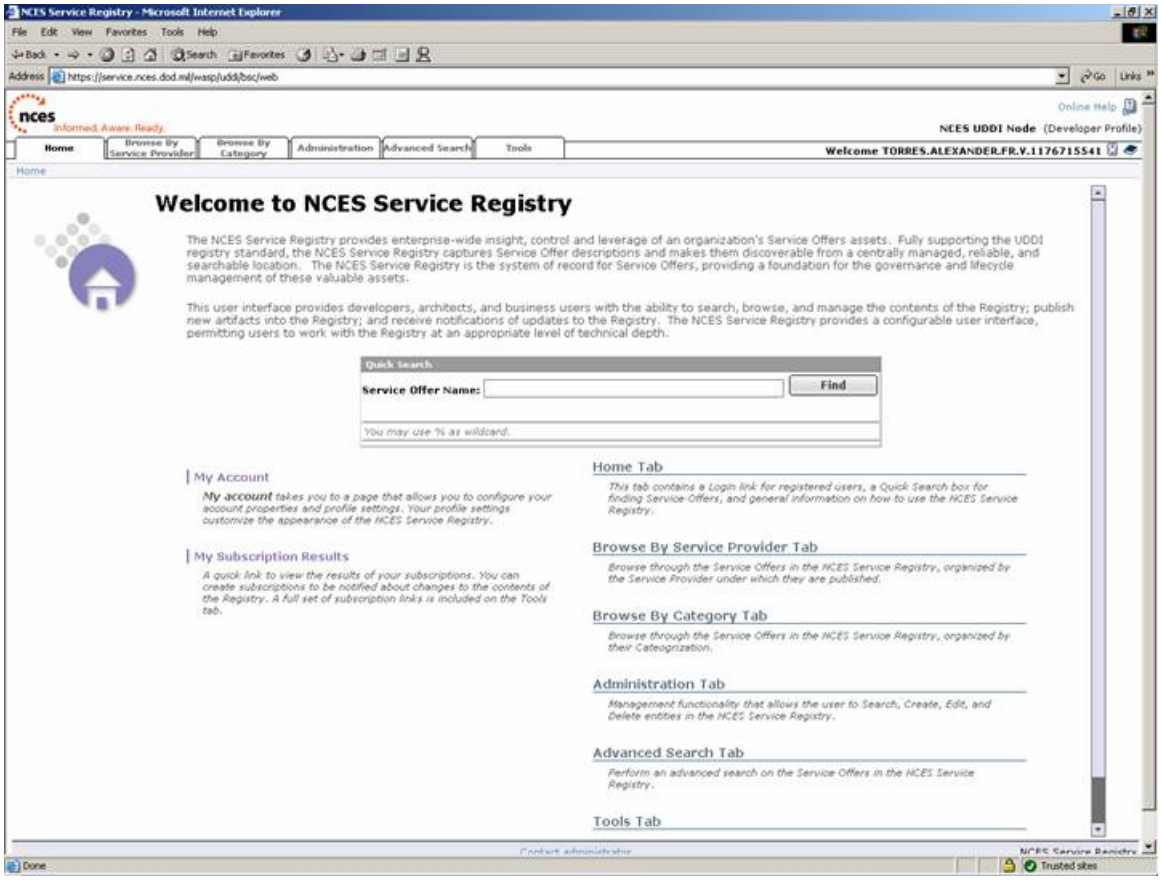

Figure 3-2. NCES Service Registry

The NCES Service Registry provides a configurable user interface, permitting you to work with the registry at an appropriate level of technical depth. The Home, Browse By Service Provider, Browse By Category, and Advanced Search tabs provide several ways to browse for services. To perform a quick search for service offers, click on the Home tab and enter the service offer name in the Quick Search box or click on the Advanced Search tab to perform an advanced search based on a combination of the service offer name and other attributes. Clicking on the Browse By Service Provider tab or Browse By Category tab enables you to browse service offers by the service provider name under which they are published or by category, respectively.

Note: The percent symbol % may be used as the wildcard character while filling the search criteria fields.

4 Service Consumer

This section provides information for users who participate in the NCES Program as service consumers. To participate in the program, you must first register to become a Portal user (see Section 1.2).

4.1 Security Enable Your Service

Figure 4-1 illustrates the steps for downloading and deploying a sample application that uses the Service Security Software Development Kit (SDK). These steps prepare you, as a service consumer, for developing applications using the Service Security SDK.

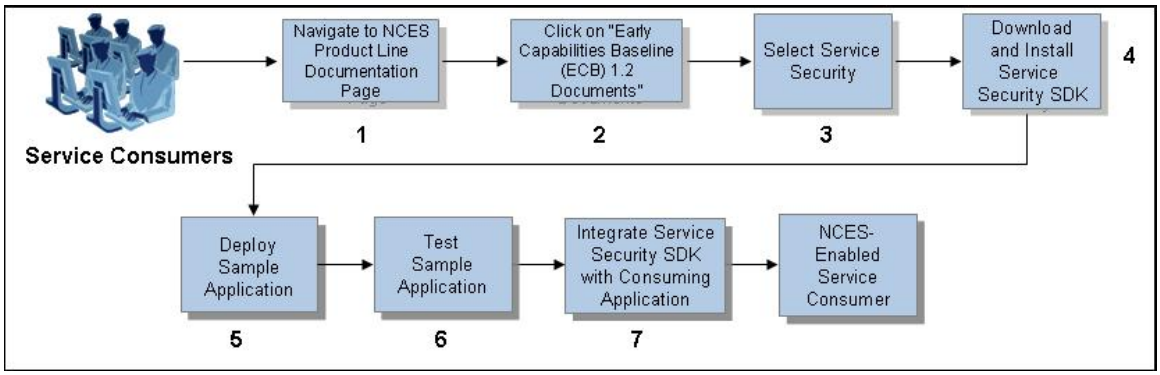

Figure 4-1. Steps for enabling Service Security

Step 1. Navigate to NCES Product Line Documentation Page
Go to https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

Step 2. Click on "Early Capabilities Baseline (ECB) 1.2 Documents"

Step 3. Select Service Security
The Service Security folder contains the NCES Service Security SDK (including Java and .Net SDKs), the NCES Service Security SDK User's Guide, the Data Gathering Checklist, and other documents.

Step 4. Download and Install Service Security SDK
Follow the instructions provided in the package for Service Security SDK installation.

Step 5. Deploy Sample Application
Deploy the sample application provided in the package.

Step 6. Test Sample Application
Deploy and test the sample application to ensure that the SDK is installed properly and works correctly with service security.

Step 7. Integrate Service Security SDK with Consuming Application

Integrate the consuming application with the Service Security SDK.

4.2 Consuming or Integrating with SOA Foundation Services

This section describes how you, as a service consumer, can consume or integrate with SOA Foundation Services.

4.2.1 Mediation Service

The NCES Mediation Service provides the capability to perform eXtensible Markup Language (XML) translations using eXtensible Stylesheet Language Translation (XSLT) stylesheets. The capability is oriented to software developers who are interested in using the service. Two primary workflows are associated with the XML translation capability. The first workflow is oriented to a user interested in translating XML data using a translation that is registered within the DoD Metadata Registry. The sample application provided within the SDK uses a translation that is registered within the registry. The second workflow describes how to register a new XSLT translation within the Metadata Registry. Successful completion of the steps in the first workflow is recommended before you attempt to register unique translations.

4.2.1.1 Service Mediation with Preregistered XSLT Translations

An SDK is provided to develop applications using the XML translation service. This SDK provides a minimal client application to invoke the Service Mediation capability for demonstration of use. The workflow illustrated in Figure 4-2 shows the steps for downloading the Mediation SDK and running the sample client application.

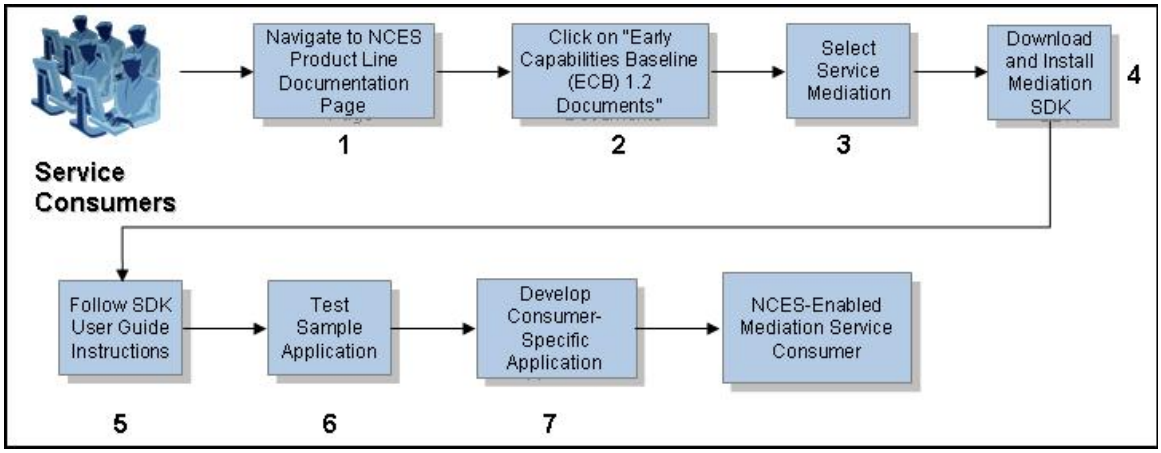

Figure 4-2. Steps for consuming Mediation Service

Steps shown in Figure 4-2 are summarized below.

Step 1. Navigate to NCES Product Line Documentation Page

Go to https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

Step 2. Click on "Early Capabilities Baseline (ECB) 1.2 Documents"

Step 3. Select Service Mediation
Select the Service Mediation folder that contains the NCES Mediation Service SDK.

Step 4. Download and Install Mediation SDK
The "NCES-mediation-SDK0.5.0-windows" zip file contains documentation libraries and a sample application to demonstrate Mediation Service usage. Follow the instructions provided in the package to install the Mediation SDK.

Step 5. Follow SDK User Guide Instructions
Consult the SDK User Guide in the SDK zip file for details on how to perform the needed configuration. Instructions are provided for calling a sample application that demonstrates the use of the Service Mediation capability.

Step 6. Test Sample Application
Run the sample application according to SDK User Guide instructions. Verify the functionality of the sample application.

Step 7. Develop Consumer-Specific Application
You are now ready to develop an application using Service Mediation services. See the enclosed sample client code and Mediation Application Program Interface (API) manuals (located in the SDK) for guidance on how to invoke the services provided.

4.2.1.2 Registering New Translations Within the DoD Metadata Registry

The workflows described in this section are for service consumers who want to register their own translations within the DoD Metadata Registry for use by the XML translation service. Guidance is provided on how to register information resources, such as XML translations and schemas, in the Metadata Registry. The information in this section provides a high-level understanding of the process of registering XML translations, which is illustrated in Figure 4-3. Detailed steps for building a submission package are available within the Mediation SDK.

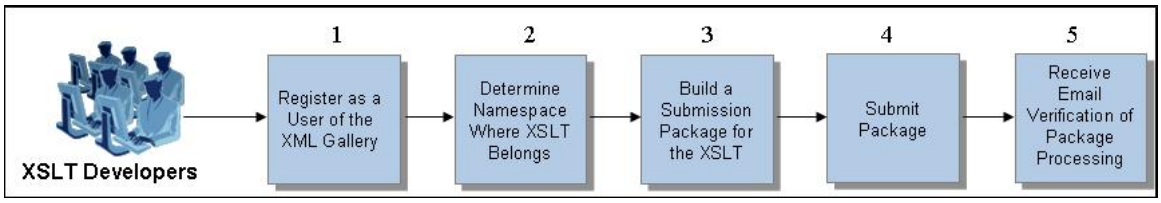

Figure 4-3. Registering an XML Stylesheet Language Translation

Step 1. Register as a User of the XML Gallery
Follow the registration link/pulldown at http://diides.ncr.disa.mil (NIPRNet) or at http://diides.ncr.disa.smil.mil (SIPRNet) for instructions on becoming a registered user of the XML Gallery.

Step 2. Determine Namespace Where XSLT Belongs
All information resources, including XSL translations, must be associated with a namespace within the DoD Metadata Registry. For testing purposes, use the "QLI" namespace. See the DoD Metadata Registry Portal for guidance on namespace usage.

Step 3. Build a Submission Package for the XSLT
A submission package contains the information resources and the metadata about the XSL translation being registered. The steps for building a submission package appear in Figure 4-4. Refer to the SDK for additional guidance on building a submission package.

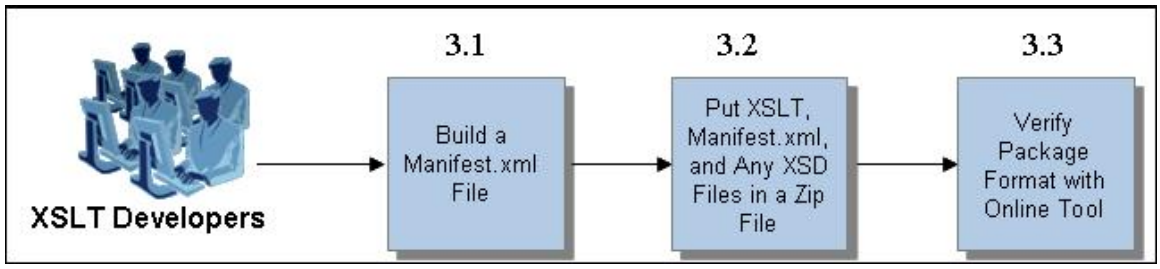

Figure 4-4. Steps for Building a Submission Package for the XSLT

- **Step 3.1. Build a Manifest.xml File**

  This step, from Figure 4-4, contains three substeps, as shown in Figure 4-5.

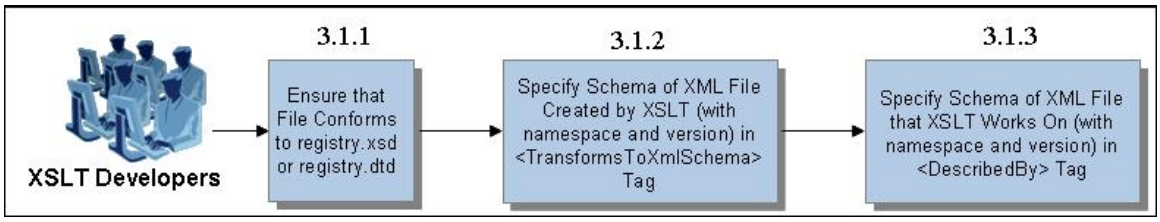

Figure 4-5. Steps for Building a Manifest.xml File

  - **Step 3.1.1. Ensure that File Conforms to registry.xsd or registry.dtd**
  - **Step 3.1.2. Specify Schema of XML File Created by XSLT (with namespace and version) in <TransformsToXmlSchema> Tag**
  - **Step 3.1.3. Specify Schema of XML File that XSLT Works On (with namespace and version) in <DescribedBy> Tag**

- **Step 3.2. Put XSLT, Manifest.xml, and Any XSD Files in a Zip File**
- **Step 3.3. Verify Package Format with Online Tool** (located on the DoD Metadata Registry Portal)

Step 4. Submit Package
The DoD Metadata Registry Portal provides an online package submission capability. The capability prompts you for the location of the submission package on the local computer. Log on to the Metadata Registry and follow the links to the online submission capability.

Step 5. Receive Email Verification of Package Processing
You should receive an email notifying you that the package has been accepted into the Metadata Registry. Confirm that you have received this email.

4.2.2 Messaging

This section describes the steps (see Figure 4-6) for using the Messaging capabilities.

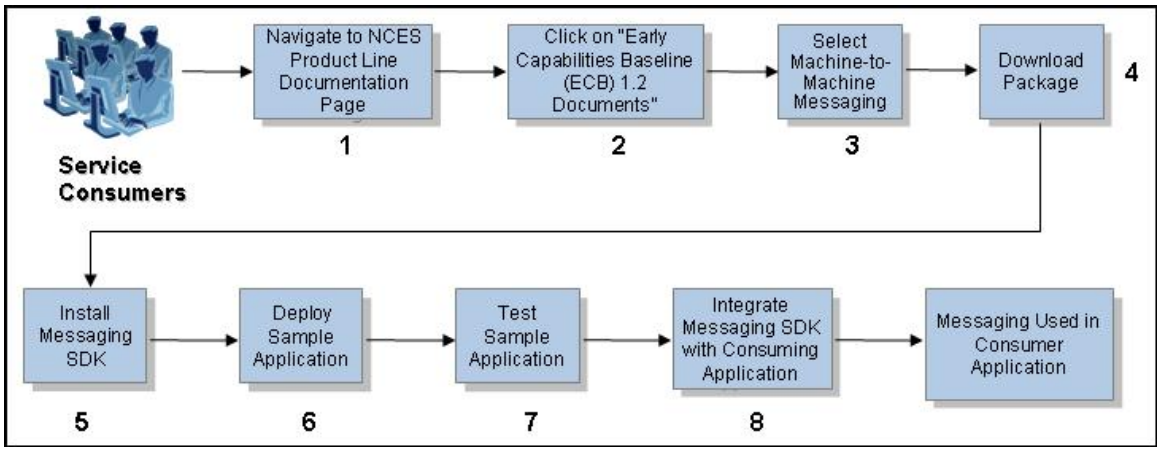

Figure 4-6. Steps for Consuming the Messaging Service

Step 1. Navigate to NCES Product Line Documentation Page
Go to https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

Step 2. Click on "Early Capabilities Baseline (ECB) 1.2 Documents"

Step 3. Select Machine-to-Machine Messaging
Select the Machine-to-Machine Messaging folder that contains the Messaging SDK

Step 4. Download Package
The Messaging SDK package contains documentation about the NCES Messaging service and a set of sample applications demonstrating its functionality. The documentation includes an overview of the Messaging service, a developer's guide that discusses technical details (such as the service specifications used), and a guide to the Messaging SDK that provides details on the sample applications. The sample applications, which exercise the functionality of the Messaging service, are already integrated with NCES service security and only require a valid certificate and configuration of the proper roles for the certificate's domain name.

Step 5. Install Messaging SDK
Unzip the Messaging SDK in a directory on the host machine. The sample applications are written in Java and will run on most operating systems. For convenience, a set of Microsoft Windows batch scripts is provided for running the various applications.

Step 6. Deploy Sample Application
The sample applications may be used to publish messages and subscribe to message channels. The applications enable developers to understand the operation of the Messaging service before integration into new applications.

Step 7. Test Sample Application
You may use the sample applications to test the configuration of the Messaging SDK. A valid PKI certificate must be obtained and installed for the applications to operate correctly. In addition, the NCES identity store must be configured with the proper roles for the certificate's domain name. Testing these configurations using the sample applications provides a controlled means to test your environment.

Step 8. Integrate Messaging SDK with Consuming Application
Because the Messaging SDK provides source code for the sample applications, the sample applications provide examples for the development of new consumer applications or the integration of messaging functionality into existing consumer applications.

4.3 Consuming or Integrating with NCES Content Discovery and Delivery Services

This section describes how you, as a service consumer, can consume or integrate with NCES Content Discovery and Delivery services.

4.3.1 Federated Search

Figure 4-7 presents the steps for using the Federated Search capabilities of NCES services.

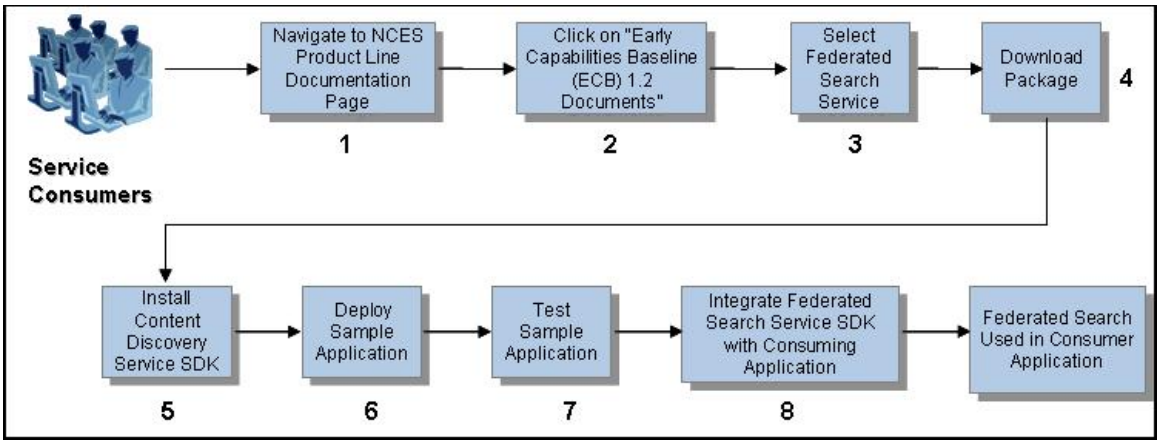

Figure 4-7. Steps for Consuming Federated Search Service

Steps shown in Figure 4-7 are as follows.

Step 1. Navigate to NCES Product Line Documentation Page
Go to https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

Step 2. Click on "Early Capabilities Baseline (ECB) 1.2 Documents"

Step 3. Select Federated Search Service
Select the Federated Search Service folder that contains the Content Discovery SDK

Step 4. Download Package
The package contains documentation and sample applications for the NCES Content Discovery services, which includes both the NCES Federated Search and NCES Enterprise Catalog services. The documentation consists of an overview of the NCES Content Discovery services, a developer's guide that discusses the details of the service specifications, and an SDK guide that discusses installation and utilization of the sample applications in the SDK.

Step 5. Install Content Discovery Service SDK
Unzip the SDK in a directory. The sample applications have been tested using Java JDK 1.4.2.

Step 6. Deploy Sample Application
The SDK documentation outlines how to configure and utilize the sample applications to access the NCES Content Discovery service.

Step 7. Test Sample Application
Once configured, you can use the sample NCES Content Discovery applications to submit queries to the enterprise. A successful test of the application demonstrates the correct configuration of the certificates and roles for NCES security services.

Step 8. Integrate Federated Search Service SDK with Consuming Application
The sample applications provide source code, which enables you to develop new applications or integrate Content Discovery capabilities into existing applications.

4.3.2 Enterprise Catalog

Figure 4-8 presents the steps for using the Enterprise Catalog service.

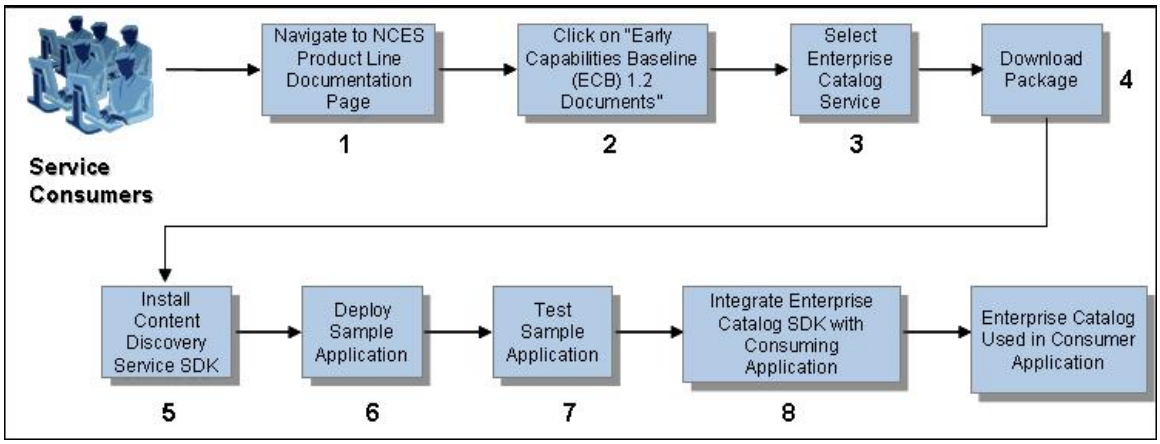

Figure 4-8. Steps for Consuming Enterprise Catalog Service

Step 1. Navigate to NCES Product Line Documentation Page
Go to https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

Step 2. Click on "Early Capabilities Baseline (ECB) 1.2 Documents"

Step 3. Select Enterprise Catalog Service
Select the Enterprise Catalog Service folder that contains the Content Discovery SDK

Step 4. Download Package
The package contains documentation and sample applications for the NCES Content Discovery services, which includes both the NCES Federated Search and NCES Enterprise Catalog services. The documentation consists of an overview of the NCES Content Discovery services, a developer's guide that discusses the details of the service specifications, and an SDK guide that discusses installation and utilization of the sample applications in the SDK.

Step 5. Install Content Discovery Service SDK
The SDK may be unzipped in a directory. The sample applications have been tested using Java JDK 1.4.2.

Step 6. Deploy Sample Application
The SDK documentation outlines how to configure and utilize the sample applications to access the NCES Content Discovery service.

Step 7. Test Sample Application
Once configured, the Service Consumer can use the sample NCES Content Discovery applications to submit queries to the enterprise. A successful test of the application demonstrates the correct configuration of the certificates and roles for the NCES security services.

Step 8. Integrate Enterprise Catalog SDK with Consuming Application
The sample applications provide source code, which allows the Service Consumer to develop new applications or integrate Enterprise Catalog capabilities into existing applications.

4.4 Consuming Customer-Provided Services

Customer-provided services will be identified through Service Discovery and consumed via the WSDL-defined interface or the integration of Service Provider SDKs.

5 Service Provider

This section provides information for individuals who participate in the NCES Program as service providers. To participate in the program, you must first register to become a Portal user (see Section 1.2).

5.1 Publish, Use, and Integrate with SOA Foundation Services

5.1.1 Service Discovery and Security Integration

The workflow illustrated in Figure 5-1 describes how you, as a service provider, can register your services and use NCES Service Security.

Note: The NCES Administrator completes Steps 3 and 9 (indicated in gray type in Figure 5-1).

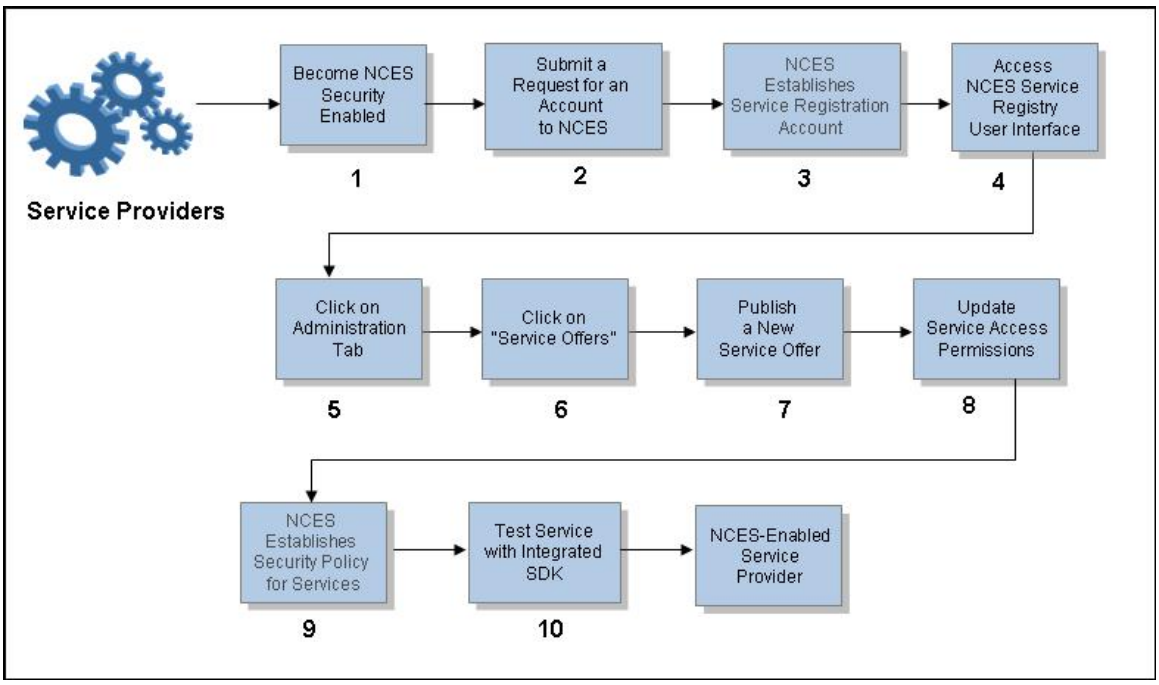

Figure 5-1. Service Provider Workflow

Step 1. Become NCES Security Enabled
Follow the workflow in Section 4.1 to become NCES security enabled.

Step 2. Submit a Request for an Account to NCES
Submit a request for an NCES account via email (nces@cols.disa.mil). Indicate that you want to publish a Web service to the NCES Service Registry and include the following information:

- Name (name on the common access card or external certificate authority (ECA) certificate)
- Phone number
- Email address

- Agency/organization
- Program you are currently working on
- Community of interest/business entity
- Names/descriptions of services you want to register

Note: The NCES Administer completes Step 3.

Step 3. Establish NCES Service Registration Account
After the NCES Administrator establishes your account, he or she will perform the following tasks:

- Create security roles (Service Discovery Administrators, Security Administrators, and/or Analysts) in the Service Security LDAP server
- Create your business entity in universal description discovery and integration (UDDI) registry
- Establish permissions so that you can publish and manage your services

Step 4. Access NCES Service Registry User Interface

Follow the workflow in Section 2.2 to go to the NCES Services Interface, which is shown in Figure 5-2. Click on the "SOA Foundation" tab and select Service Discovery from the drop-down menu.

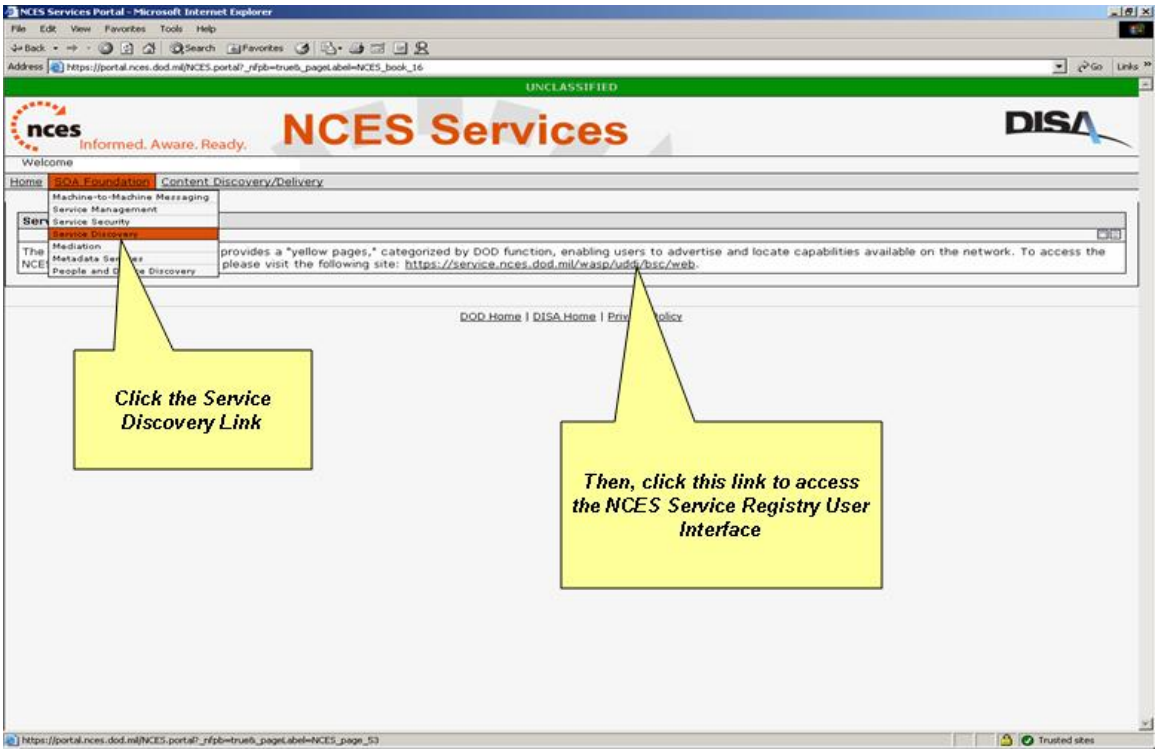

Figure 5-2. NCES Services Interface

Click on the link https://service.nces.dod.mil/wasp/uddi/bsc/web to access the NCES Service Registry, which is shown in Figure 5-3.

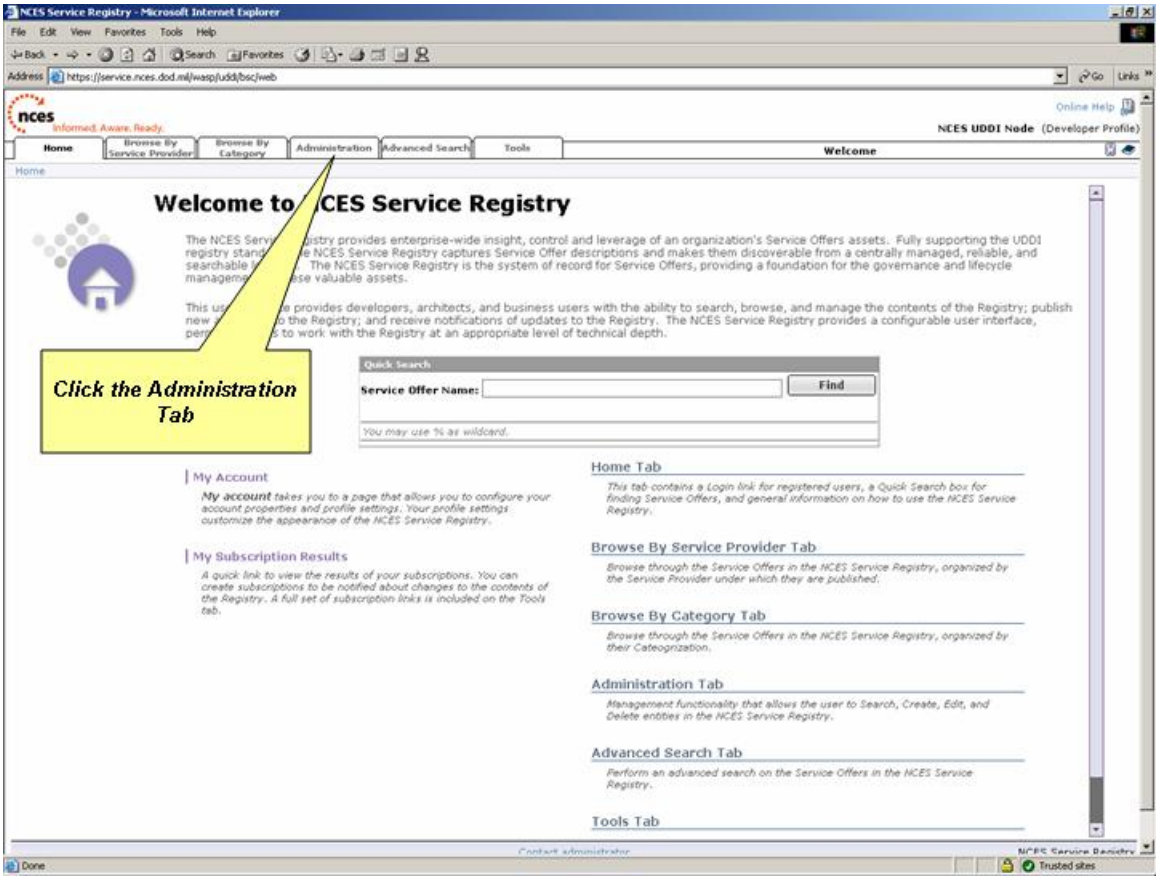

Figure 5-3. NCES Service Registry

Step 5. Click on Administration Tab

Step 6. Click on "Service Offers"

- Click on "Service Offers" in the NCES Service Registry User Interface, which is shown in Figure 5-4.

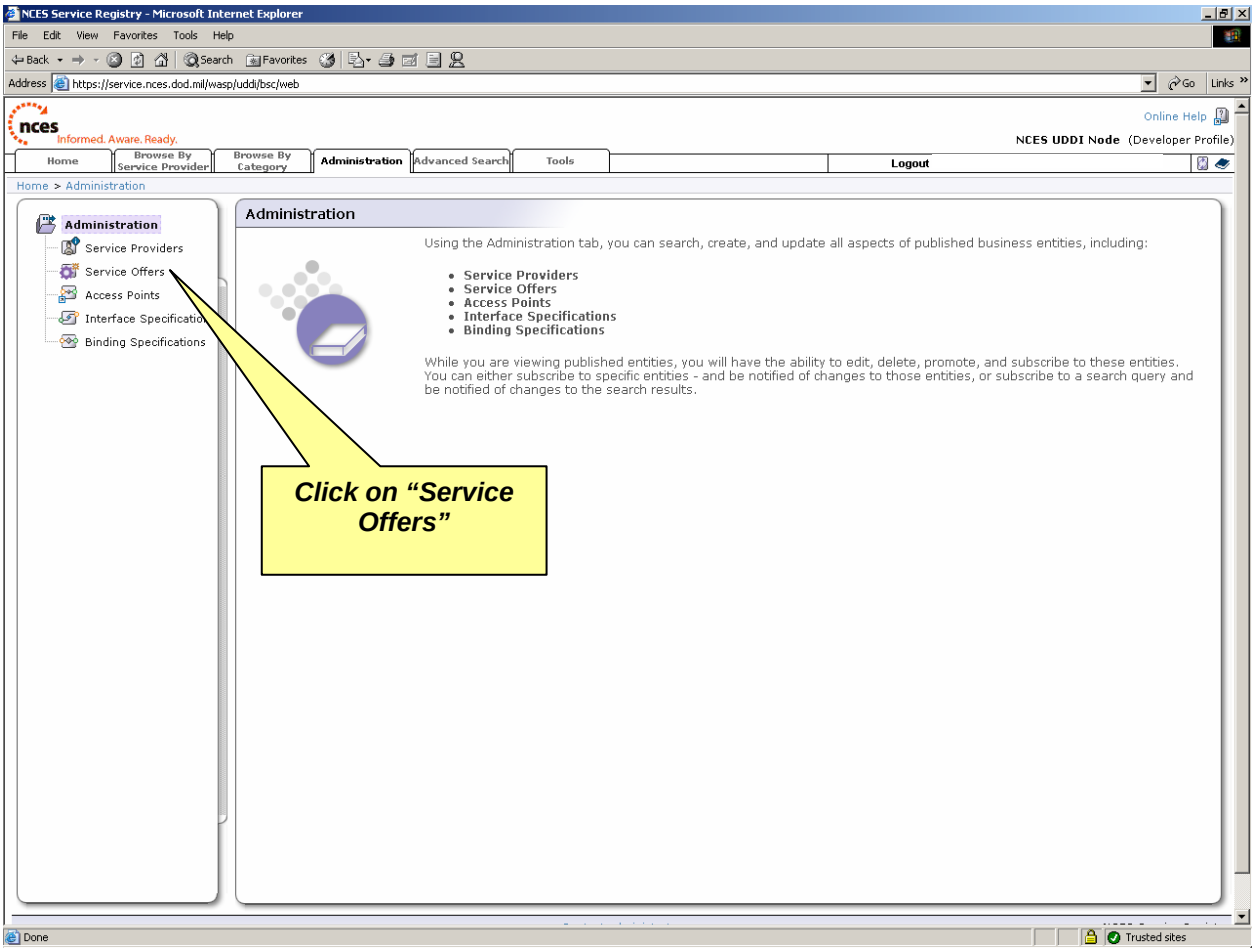

Figure 5-4. NCES Service Registry User Interface

In the "Service Offers" area, you can accomplish the following:

- View all published service offers
- Create a search query for service offers
- Manage (edit or delete) published services
- Publish a new service offer (see Step 7)

Step 7. Publish a New Service Offer

You may publish a new service offer by listing the appropriate endpoint in the NCES Service Registry. A unique name will be given to the service based on the Qualified Name (Qname) of the WSDL. Choose a name from the list of registered service providers and provide the WSDL location. The unique name will be the basis used by NCES Service Security to enforce security policies.

Note: The "NCES Service Discovery CONOPS [Concept of Operations] v0.5" (pages 23–41) and "UDDI Publishing Guide" (pages 23–38) are useful references for publishing new service offers and managing published service offers. To download these documents, go to https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or

https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet). Click on the "ECB 1.2 Documents" bar and select the Service Discovery folder.

Step 8. Update Service Access Permissions
You are authorized to edit or delete your published services. Updating your service access permissions enables you to delegate the administration of your services to user groups. Five permissions are associated with service administration:

1. **Find Service:** To find the service in the registry
2. **Get Service:** To get detailed information on the service
3. **Save Service:** To update and save the service information
4. **Delete Service:** To delete the service and its endpoints from the registry
5. **Create Endpoints:** To create new endpoints for the service

Note: The NCES Administrator completes Step 9.

Step 9. Establish Security Policy for Services
To mitigate security risks, the NCES Administrator is responsible for establishing access control policies for service providers and their user groups.

Step 10. Test Service with Integrated SDK
Verify that the service functions properly after it is integrated with Service Security.

6 Data Provider

This section provides information for individuals who participate in the NCES Program as data providers. To participate in the program, you must first register to become a Portal user (see Section 1.2).

6.1 Content Discovery and Delivery

Content Discovery and Delivery is used to query existing data sources, such as databases, catalogs, and search engines, to quickly find stored information. As a data provider, you can use the Enterprise Catalog service to publish metadata about a data source, and the metadata can then be searched using the Content Discovery Federated Search Portlet. If a user wants to access your data, the data will be retrieved and delivered using Content Delivery. The Enterprise Catalog service can be accessed using the Web service client distributed with the NCES Content Discovery SDK. Alternatively, you may directly implement the Federated Search Web Service and integrate directly with the NCES Content Discovery service.

6.1.1 Publish Content Using NCES Content Discovery

The Enterprise Catalog service is capable of submitting and indexing DDMS metadata to data sources. As a data provider, you may submit metadata to the service, which stores the data for retrieval through the Content Discovery Federated Search Portlet. The Enterprise Catalog Web service can be utilized through the Enterprise Client provided with the Content Discovery SDK. Download the Content Discovery SDK from the NCES Product Line Documentation Page at https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

6.1.2 Expose Content Using NCES Content Discovery

The Federated Search Web Service specification provides a standard query interface allowing NCES Content Discovery Services to submit a query to a data provider. As a data provider, you may execute the query, which returns the results containing DDMS-compliant metadata. The results are then aggregated with results returned from other data providers and returned to the user through end-user applications such as the Content Discovery Federated Search Portlet. Sample implementations of a data provider for the Federated Search Web Service will be added to the Content Discovery SDK. The Content Discovery SDK can be downloaded from the NCES Product Line Documentation Page at https://gesportal.dod.mil/sites/NCES Product Line Documentation/default.aspx (NIPRNet) or https://gesportal.dod.smil.mil/sites/NCES Product Line Documentation/default.aspx (SIPRNet).

6.2 DoD Metadata Registry Information

The DoD Metadata Registry enables you to publish metadata artifacts (e.g., schemas, stylesheets, taxonomies) to a portal available to the DoD community. Making user metadata products visible to the community enable others to reuse the user's hard work and promotes interoperability between systems. To use the services provided, the user must be a registered user on the Metadata Registry Portal. Using the user's PKI user certificate and Portal registration to access the capabilities is not supported at this time. To register as a user on the Metadata Registry Portal, follow the instructions at https://diides.ncr.disa.mil/xmlreg/user/register.cfm (NIPRNet)

or https://diides.ncr.disa.smil.mil/xmlreg/user/register.cfm (SIPRNet). The account created will provide access to the data within the portal and the ability to register new data products. The account also will provide access to the runtime APIs for application access to the metadata products.

Metadata products are registered in the Metadata Registry by creating a submission package and submitting the package file. Details on building a submission package, using package creation tools, validating the package, and submitting a package are available at http://diides.ncr.disa.mil/xmlreg/user/information.cfm#submit (NIPRNet) or http://diides.ncr.disa.smil.mil/xmlreg/user/information.cfm#submit (SIPRNet). If a user encounters problems accessing the DoD Metadata Registry, he or she can submit questions or provide feedback at http://diides.ncr.disa.mil/xmlreg/user/feedback.cfm (NIPRNet) or http://diides.ncr.disa.smil.mil/xmlreg/user/feedback.cfm (SIPRNet). Registered users of the Metadata Registry can access the DoD Metadata Registry Portal at http://metadata.dod.mil.

The DoD Metadata Registry also provides Web Services access to locate XSL translations between XML schemas at runtime. Section 4.2.1 describes the workflow for discovering and using a registered XSL translation. The WSDL for this service is available at http://diides.ncr.disa.mil:7001/mediation/MediationService?WSDL (NIPRNet) or http://diides.ncr.disa.smil.mil:7001/mediation/MediationService?WSDL (SIPRNet).

7 For More Information

For general information about NCES, go to the following:

- NIPRNet: https://dol.dod.mil or https://www.nces.dod.mil (NIPRNet)
- SIPRNet: https://dol.dod.smil.mil or http://www.nces.dod.smil.mil

For technical support, contact the NCES Technical Assistance Center, which operates 24 hours a day, 7 days a week:

- Phone: (800) 447-2457 (toll free) or (614) 692-3136
- DSN: 850-3136
- Classified Phone: Please contact the unclassified phone number listed above and request a call back on a classified line.
- Unclassified Email: nces@cols.disa.mil
- Classified Email: nces@roscc.disa.smil.mil
- Unclassified/Nonsecure Fax: (614) 692-2505
- Classified/Secure Fax: (614) 692-9988

DoD PKI Help Desk:

- (800) 490-1643, option 5 (toll free)
- Unclassified Email: weblog@chamb.disa.mil

Appendix A. Acronyms

API	Application Program Interface
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ATC	Authority to Connect
ATO	Authority to Operate
CL	Confidentiality Level
DAA	Designated Approval Authority
DDMS	Department of Defense Discovery Metadata Specification
DISA	Defense Information Systems Agency
DoD	U.S. Department of Defense
DOL	Defense Online
DSN	Defense Switched Network
ECB	Early Capabilities Baseline
GES	Global Information Grid Enterprise Services
GIG	Global Information Grid
IM	Instant Messenging
JDK	Java Developer Kit
LDAP	Lightweight Directory Access Protocol
MAC	Mission Assurance Category
NCES	Net-Centric Enterprise Services
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QName	Qualified Name
QRG	Quick Reference Guide
RSS	Rich Site Summary
SDK	Software Development Kit
SIPRNet	Secret Internet Protocol Router Network
SOA	Service-Oriented Architecture
UDDI	Universal Description Discovery and Integration
WG	Working Group
WIPT	Working-level Integrated Product Team
WSDL	Web Services Description Language
XML	eXtensible Markup Language
XSD	XML Schema Definition
XSL	eXtensible Stylesheet Language
XSLT	eXtensible Stylesheet Language Translation

Appendix B. Mission Assurance Categories and Confidentiality Levels

The following definitions of Mission Assurance Category (MAC) and Confidentiality Level (CL) are taken from DODI 8500.2.

Confidentiality Level. Applicable to U.S. Department of Defense (DoD) information systems, the confidentiality level (CL) is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). DoD has three CLs: classified, sensitive, and public.

Mission Assurance Category. Applicable to DoD information systems, the Mission Assurance Category (MAC) reflects the importance of information to the achievement of DoD goals and objectives, particularly the Warfighters' combat mission. MACs are primarily used to determine availability and integrity requirements. DoD has three MACs:

- **MAC I.** This category consists of systems that handles information that is vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

- **MAC II.** This category consists of systems that handle information that is important for supporting deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can be tolerated for a short time only. The consequences could include delay or degradation in providing important support services or commodities, which could seriously impact mission effectiveness and/or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure mission assurance.

- **MAC III.** This category consists of systems that handle information that is necessary for the conduct of day-to-day business but that does not materially affect support to deployed or contingency forces in the short term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

This page has been left blank intentionally.